Understanding Data Remanence in Automated Systems, September 1991. Additional procedures are described in DoD 5200.28-M, ADP Security Manual, January 1973.

l. Information Sensitivity Designation.* DISA information systems will be assigned an information sensitivity designation based upon their highest classification or sensitivity. Assets that are designated as classified require protection as mandated in DoD 5200.1-R, Information Security Program Regulation (reference 4a). Assets designated Sensitive but Unclassified require protection by virtue of law, federal statute, regulation, or when its disclosure, modification, or destruction would impact the DISA mission. Nonsensitive assets do not require stringent protection and, if destroyed or rendered unavailable, will not affect DISA's ongoing operational mission nor subject DISA to unwarranted legal action or create risk to the national security.

m. Information System Security Officer (ISSO).* An ISSO will be appointed for a single system or cluster of information systems. For information systems undergoing development, the ISSO will function as the Application Security Engineer (ASE) responsible for designing security into life-cycle development. The ISSO/ASE should ensure that effective security products and techniques are appropriately used in the information system and should be contacted when security incidents or violations occur.

n. Personnel Controls. Automated or manual controls will be implemented to enforce individual accountability, least privilege, and the separation of duties among users of an information system. Safeguards will be implemented to restrict users to information or functions to which the user is entitled (by virtue of clearance, formal access approval, or job title), but to no more. In the case of "need-to-know" for classified information, access must be essential for accomplishment of lawful and authorized U.S. Government purposes.

o. Personnel Security Controls. Controls will be established to screen personnel who have access to an information system or to its information. Guidance regarding personnel security investigations can be found in DISAI 240-25-6, DISA Personnel Security Program, 24 January 1983. Individuals occupying information system processing positions will be designated as ADP-I, ADP-II, or ADP-III. Individuals with the capability to bypass security as part of their interaction with an information system, such as the ISSO or System Administer, will be designated as ADP-I and be investigated accordingly.

p. Physical Controls.* Procedures will be established to protect the information, its hardware, software, and documentation from unauthorized disclosure, destruction, or modification. The level of control and protection shall be commensurate with the maximum sensitivity level of the information and will include the security disciplines, administrative

procedures, and configuration controls necessary to ensure availability of the information system.

q. Physical Security Controls. Controls will be implemented to adequately protect facilities, personnel, equipment, and sensitive information. Minimum physical security requirements may be obtained from CISS.

r. Reporting of Security Violations and Computer Security Incidents.* Procedures will be established to ensure the reporting of security violations as required by DISAI 240-110-8, Information Security Program (reference 4b). Security incidents, whether caused by computer viruses, hackers, or software bugs will be considered in the development of these procedures and will be reported to the local information system security officials and to the DISA Automated Systems Security Incident Support Team (ASSIST) Branch. ASSIST can be reached via e-mail at assist@assist.mil. Procedures will be developed for the reporting of security incidents for nonsensitive systems.

s. Risk Management. A risk management program will be developed to periodically review and assess the implemented security controls. The program will determine the effectiveness of the protection currently afforded and will assess what additional protective measures are needed to achieve an acceptable level of operating risk based upon the identified threats.

t. Security Education and Awareness Program. A security education and awareness program, specific to the use and operation of the information system, will be established to provide mandatory, periodic, and refresher training. Users will be trained in the specific security features of the information system and will be provided the rules regarding acceptable use and operation.

u. Security Mode of Operations. The planned or implemented system security mode of operation must be defined. The system mode of operation is determined by completing the risk index tables identified in Enclosure 4 of the authority document, DoDD 5200.28 and is based on the sensitivity level of the data, the personnel security clearance or investigation of the users, and the user's need-to-know. The different modes of operation are: Dedicated Mode; System High Mode; Multilevel Mode; and Multilevel, Partitioned Mode.

5. Noncompliance. Information systems that fail to meet the minimum requirements and have not received an exemption will be

denied accreditation. The cognizant Functional Application OPR or the General Support System OPR will terminate all system operations upon receipt of the Statement of Termination issued by the Director or Vice Director.

Section C. MAJOR APPLICATIONS AND GENERAL SUPPORT SYSTEMS

6. General. Major Applications and General Support Systems, as identified in authority document OMB Circular A-130, are the two types of systems used throughout DISA. The difference between the two is that a Major Application establishes and implements security requirements for the express purpose of protecting the information while a General Support System establishes and implements security requirements for the purpose of protecting the system and its operating environment. There is no significant difference in the level of effort required to protect a Major Application versus a General Support System. This section specifically outlines the security requirements applicable to both Major Applications and General Support Systems and identifies additional security requirements specific for each type of system. Organizations will consult the security controls and requirements described in both section B and this section.

7. Security Requirements for Major Applications and General Support Systems. For major applications, the controls of the General Support System(s) in which they operate are likely to be insufficient. Therefore, additional controls specific to the application are required. The cognizant Functional Application OPR will establish the minimum requirements necessary to ensure that adequate security is provided for all information processed, stored, or transmitted within their systems. Requirements described below apply to both Major Applications and General Support System environments.

a. Assignment of Responsibility for Security. An ISSO will be appointed for individual systems or groups of information systems. For a Major Application, the ISSO will function as an Application Security Engineer (ASE) and should be knowledgeable with the nature of the information processed by the application to assist in its secure design and the selection of management, operational, and technical controls needed to protect it. The ISSO for a General Support System must possess a broader knowledge of the information security technology employed in the General Support System environment and any inherent security vulnerabilities.

b. Development of a Security Plan. IAW the authority document, the Computer Security Act of 1987, each Major Application or General Support System that processes sensitive (classified or sensitive but unclassified) information will have a security plan. DISA has developed a standardized system security plan (SSP) that is compliant with OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for

Federal Computer Systems that Contain Sensitive Information (reference 4c). The DISA Information System Security Plan (depicted in figure 3-1) is the format to be used when developing SSPs.

c. Development of Guidance Regarding Acceptable User Behavior. Guidance should be as stringent as necessary to provide adequate security and to clearly delineate responsibilities and describe expected behavior of all individuals with access to the application. Additionally, guidance should be clear about the consequences of behavior that is not consistent with use of the information technology. For General Support Systems, guidance should also cover topics such as dial-in access, connection to the INTERNET, use of copyrighted software, obtaining system access, and unofficial use of government technology assets.

d. Development of a Program for Security Awareness and Training. A program will be established to ensure that all individuals receive specialized awareness training that is focused on their responsibilities and application rules before being allowed access to the application. This may be in addition to awareness and training required for access to a system. Such awareness training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high risk application).

e. Implementation of a Personnel Security Program. The Personnel Security Program should incorporate controls such as separation of duties, least privilege, and individual accountability into the application, as appropriate. In cases where such controls cannot adequately protect the application and information, position sensitivity must be designated to determine the level of background investigation that is commensurate with the risk and magnitude of the harm they could cause. The Functional Application OPR or General Support System OPR should designate ADP sensitivity of positions for individuals who are authorized to bypass technical and operational security controls of the system (e.g., LAN administrators or system programmers). Such screening should be done prior to the individuals being authorized to access the application and periodically thereafter.

f. Development of Test Plans for Continuity of Operations. For Major Applications, establish and periodically test the capability to perform the function supported by the application in the event of an application or system failure. For General

Support Systems, periodic testing should occur to ensure that service provided by the system can be continued based upon the needs and priorities of the participants of the system.

g. Implementation of Technical Security Controls. For Major Applications, ensure that appropriate security controls are specified, designed into, tested, and accepted. For General Support Systems, ensure that cost-effective security products and techniques are appropriately used within the system.

h. Assessment of the Effectiveness of Security Controls. For Major Applications operating within a General Support System, additional security controls specific to the application are required. The cognizant Functional Application OPR will establish the minimum requirements necessary to ensure that adequate security is provided for all information processed, stored, or manipulated by the application. An independent review or audit of the security controls in each application should be conducted at least every 3 years. The review should support reaccreditation activities, ensure that deficiencies are documented and repaired, and provide an update to the cognizant ISSO on the effectiveness of the applications security controls. For General Support Systems, a review of the security controls in each system should be conducted when significant modifications are made and at least every 3 years. The review should identify that the security controls are commensurate with the acceptable level of risk for the system.

i. Correction of Technical Vulnerabilities Associated with Commercial, Off-The-Shelf Products (COTS). A process must be developed to incorporate recommendations to correct technical vulnerabilities that impact the security of an information system. Such recommendations are posted in Automated Systems Security Incident Support Team (ASSIST) Bulletins. The process must cite the bulletin number, the date that the security patch or fix was made, and the name of the individual who performed the correction. Reports or bulletins regarding a technical vulnerability does not necessarily mean that an actual violation or security incident has occurred. However, the potential for exploitation does exist, and the technical vulnerability should be corrected in a timely manner. Procedures must be established to ensure that the ASSIST Bulletin Board or other advisory bulletin boards (i.e., Computer Emergency Response Team [CERT]) are reviewed periodically to gather information on identified technical vulnerabilities.

j. Accreditation. The requirements described in chapter 3 must be met to obtain accreditation. Reaccreditation is merited at least every 3 years or whenever a major change occurs.

TO BE USED FOR THE COMMUNICATIONS, TRANSMISSION, PROCESSING, MANIPULATION, AND STORAGE OF OFFICIAL U.S. GOVERNMENT OR OTHER AUTHORIZED INFORMATION ONLY. UNAUTHORIZED USE OF THIS COMPUTER MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

d. Marking.

(1) Output Marking. Automated or manual procedures will be developed to mark or accurately reflect the sensitivity or classification of the information being processed. Automated markings of output cannot be relied on to be accurate unless the security features and assurances of the information system meet the requirements for a minimum security class of B1, as specified in DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985. If class B1 is not met, but automated controls are used, all output shall be protected at the highest classification level of information handled by the information systems until manually reviewed by authorized personnel to ensure that the automated markings are accurate.

(2) Equipment Marking. All information systems that process classified information will be marked with the highest classification level of information being processed and stored. The equipment must be marked so that it can be easily read from a minimum distance of 10 feet. Some examples of marking methods are tags or classified document cover sheets. Systems that process both classified and unclassified information must have their equipment clearly marked according to the level of information being processed or stored, to include unclassified information.

e. Automatic Lock Out. Systems using automated access controls must lock users out after a predetermined number of sequential failed logon attempts. Restoral of user access after lockout shall require manual intervention by authorized personnel. For Major Applications and General Support Systems designated as mission-critical or those systems that process information classified higher than Secret, automatic lockout must occur after not more than two logon attempts. For all other systems, the lockout must occur after a maximum of three logon attempts.

f. Automatic Timeouts. All systems that process sensitive information will have a "timeout" protection feature that automatically terminates the user session after a predetermined period has passed without communication between the user and the system. The timeout feature may not be required if the DAA determines that the system must remain active as a communications device. However, physical security for the system will meet the requirements for storage of data at the highest level that could be received. The time period may vary, depending on the sensitivity of the data, but should not exceed 15 minutes.

8. Requirements Specific to Major Applications.

a. Information Sharing. Specific requirements must be developed to ensure that information, when shared with other applications, can be protected consistent with the guidelines (i.e., security policy) developed for the information when it is processed within the application.

b. Public Access Controls. Where the application promotes or permits public access, additional security controls should be added to protect the integrity of the application. Such controls should include segregating public accessible information from official agency records and employing techniques such as access control lists, permissions by group or domain, and separations either logical or physical.

c. Data Integrity. Safeguards used by the information system must be able to detect and minimize unauthorized modification or destruction of data. Safeguards shall ensure that DISA information and assets are protected from the potentially destructive impact of human error (inadvertent actions) as well as malicious logic and unauthorized modification of hardware, software, or data.

9. Requirements Specific to General Support Systems.

a. Incident Response Capability. Develop criteria to assist users in identifying computer security incidents (e.g., virus contamination, intruder attacks). Guidance should also be developed to allow for the reporting of these incidents and the sharing of information concerning common vulnerabilities and threats. Computer security incidents must be reported to the local site ISSM/ISSO and to the DISA ASSIST at assist@assist.mil.

b. System Interconnection. Establish a Memorandum of Agreement (MOA) when interconnected systems are managed by different DAAs. The MOA should include a description and sensitivity of the information, clearance levels of the users (if required), designation of the DAA who will resolve conflicts among the DAAs, and safeguards to be employed to ensure adequate security. Where connection is authorized, controls should be established that are consistent with the rules established for the interconnecting General Support System.

c. Use of Logon Banners. All DISA information systems will display the following "logon banner" immediately upon startup and before the logon request for user ID and password. The banner shall remain displayed at least until a suitable user response (e.g., disconnect or start of login) is detected.

USE OF THIS OR ANY OTHER DEPARTMENT OF DEFENSE INTEREST COMPUTER SYSTEM (DODICS) CONSTITUTES YOUR CONSENT TO MONITORING BY DOD AUTHORIZED PERSONNEL FOR COMPUTER SECURITY AND SYSTEM MANAGEMENT PURPOSES. THIS DODICS AND ALL RELATED EQUIPMENT ARE

g. Applications Security.

(1) Control of Vendor or Custom Developed Applications. Procedures must be established for the physical and administrative control of vendor and custom developed applications under the cognizance of the local site.

(2) Application Transfers. General Support System OPRs who receive custom developed applications will establish security procedures to install, utilize, or operate such applications. The local ISSM/ISSO will review and assess the acceptability of the security documentation provided by the developing organization. As a minimum, the developing organization will provide a Security Plan, prepared IAW OMB Bulletin No. 90-08 (reference 4c), regarding the installation, operation, and maintenance of the application and a description of the existing security features. The developing organization will also submit a formal statement of accreditation.

h. Computer Security. The following requirements establish measures and controls that further ensure confidentiality, integrity, and availability of the information processed and stored within the hardware, software, and firmware components of a computer system.

(1) Configuration Management. The ISSM or designee must evaluate the impact to security for all changes (hardware, software, and firmware) to the system.

(2) Maintenance. Procedures will be established to control both on-site and remote access of personnel assigned to conduct performance maintenance. Procedures will be established to control and audit remote access and the use of remote system diagnostics under routine and emergency cases. Use of remote diagnostics is authorized for information systems that process sensitive but unclassified information only when some form of enhanced identification and authentication is used. The use of remote system diagnostics for systems that process classified information is authorized only when the transmission paths are encrypted using NSA endorsed equipment and key material and all maintenance personnel have the appropriate security clearance.

CHAPTER 3. ACCREDITATION OF DISA INFORMATION TECHNOLOGY

1. General. This chapter provides an overview of the accreditation process, outlines essential requirements, and identifies relevant organizational responsibilities. DOD policy requires that all information systems be accredited and that those systems and networks that process classified or sensitive but unclassified information be designed, developed, and implemented with appropriate security safeguards. The safeguards applied must be commensurate with the value and sensitivity of the information processed. When an adequate level of security safeguards exist, thereby satisfying the necessary security requirements, a statement of accreditation will be issued as an approval to operate. To promote understanding of the information contained within this chapter, the term "information processing asset" may apply to an information system, network, or information processing site. Guidance regarding the preparation of the System Security Authorization Agreement (SSAA) may be obtained from CISS.

2. Discussion of Terms. The terms Accreditation and Certification, often used interchangeably, are actually two separate functions that support each other. In summary, when the DAA has issued a statement of accreditation, the DAA has weighed the "evidence" provided by the Certification Authority and has decided to "accept the residual risk" of operations. The statement of accreditation is the "end state" of the initial accreditation process, but not the final state, as the risk of the accredited or approved baseline must be periodically reviewed for significant changes. Certification measures the effectiveness of the technical and nontechnical security features or attributes that have been applied. Accreditation and Certification are further defined below.

a. Accreditation. Accreditation is formally defined as the official management authorization to operate an information system. Accreditation normally grants approval to operate in a particular security mode, with a prescribed set of countermeasures (administrative, physical, personnel, COMSEC, emissions, and computer security), with stated vulnerabilities (if any), within a given operational concept and environment, with stated interconnections to other systems, within an acceptable level of risk for which the accrediting authority has assumed responsibility, and for a specified period of time (not to exceed 3 years).

b. Certification. Certification is the comprehensive evaluation of the technical and nontechnical security features and other safeguards executed, in support of the accreditation

process, to establish the extent to which a particular design, implementation, or operation meets a set of specified security requirements.

3. Accreditation Decisions. The DAA must be aware of the essential operational and security requirements along with the specific threat(s) before deciding accreditation is merited. The DAA must balance the risk of disclosure, loss, or modification of information; asset availability based on the vulnerabilities identified by the certification or technical evaluation process; the threat of exploitation of these vulnerabilities; and the operational mission requirement in order to make a decision to issue either a Statement of Accreditation, an Interim Authority to Operate (IATO), or to terminate operations. An accreditation decision is based on the degree of existing residual risk resulting from the technical or nontechnical evaluation. If the Certification Authority attests to the adequacy of the security safeguards, then the DAA must determine whether the existing residual risk is acceptable, given the organization's mission and operational environment. Key factors and accreditation decision options include:

a. Statement of Accreditation. A statement of accreditation is a formal declaration by the DAA that an information system has been approved to operate in a particular security mode using a prescribed set of safeguards. The decision to accredit is based on the residual risks identified during the certification process.

b. Interim Authority to Operate. The DAA may grant an IATO that indicates conditional approval to operate. An IATO may be issued in those situations where, due to unforeseen circumstances, the requirements for full accreditation cannot be met in a timely manner. When an IATO has been issued, the responsible organization will develop a milestone plan with dates to correct the deficiencies noted in the certification report. It is the responsibility of each organization to ensure that their information processing assets attain formal accreditation or cease operation by the expiration date of the IATO. The DAA will consider extending the period of the IATO beyond the initial period; however, no more that two IATOs will be issued.

c. Statement of Termination. If an information system's operational security risk exceeds an acceptable level, considering its operational mission and criticality, the DAA, in coordination with the operational manager, will issue a directive to terminate operations. The directive will recommend ways to improve the system's security to a minimally acceptable level for operation to resume under an IATO. The operational manager or functional proponent may appeal a directive to

terminate operations on the basis of operational necessity and the Director or Vice Director will decide on the issue within 72 hours.

4. Accreditation Approaches. Given the complexity of the asset to be accredited, its technology implementation, or nature of its operation, the DAA may require that the information system be certified and accredited in one of the following scenarios.

a. Information System. The DAA may determine that the information system undergo certification and accreditation in an environment where the system monitors and provides its own security. In this scenario, certification activities are focused on the safeguards that the system provides while the external controls (i.e., locks, guards, etc) are only identified in a cursory manner. The information system accreditation would apply to certain types of technology implementations, e.g., client-server or distributed system.

b. Type Accreditation. The DAA may approve a "type accreditation" for information systems that have similar hardware and software configuration and modes of operation and sensitivity levels and where the risk of operating in a physically secure environment is considered low. The DAA will establish the requirements and conditions under which an information system can be accredited using the type accreditation scenario.

c. Site Accreditation. The DAA may determine that a site accreditation approach is the optimal way to effect an accreditation given the number of information systems, networks, or unique operational characteristics. Test sites, Network Operations Centers (NOCs), and large data processing facilities such as MegaCenters are candidates for site accreditation. In this scenario, certification activities are focused on the safeguards that are provided by the information system and all external controls (administrative, physical, personnel, COMSEC, emissions, and computer security). Where the DAA has accredited a site, the statement of accreditation will state the approved set of countermeasures that are accredited and will specify the conditions, given the operational concept and environment, under which the site has been approved to operate.

5. Reaccreditation. Information processing assets will be reaccredited at least every 3 years or when a major change has been made that impacts security. The level of effort required for recertification and reaccreditation action will depend on the scope of the change to the security environment. Review of configuration management activities and the current environment by the DAA and certifying authority will determine actions required for reaccreditation. Reaccreditation may include the same steps accomplished for the original accreditation; however, portions of the security documentation which remain valid will

not need to be redone. The following is a representative (not all inclusive) example of events that may impact security and could require reaccreditation action. The ISSM/ISSO must submit a request for reaccreditation under the conditions that follow:

a. A change in criticality or sensitivity level of the information processed.

b. A breach of security or violation of system integrity which reveals a flaw in security design, system security management, policy, or procedure.

c. A change in the threat environment impacting overall system risk.

d. A change in the system security mode of operation.

e. A change in the operating system, security software, or hardware that affects the accredited security countermeasure implementation.

6. Accreditation Process. The accreditation process involves the collection and comprehensive analysis of security relevant information pertaining to an information system or network and a certification of the adequacy of safeguards against potential threats. Specific security requirements should be identified and an associated security concept of operations should be developed as early as possible within the system life cycle to ensure that appropriate safeguards are incorporated and that any associated risk can be managed at an acceptable level. While the responsible requesting organization will develop a significant portion of the supporting security documentation, the DISA Certification Authority will determine the breath and depth of certification activity to take place. The following high level steps outline the process and requirements and identify the responsible entity. The process to obtain accreditation does not have a predetermined timeframe (e.g., 30 days, 1 year) from beginning to completion. However, organizations should note that commitment of resources (i.e., time, people, money) will accelerate the process considerably. It should also be noted that notifying both the DAA and the Certification Authority early in process of the development of a new system, network, or site design will greatly minimize the cost of retrofitting security countermeasures, thereby greatly enhancing the possibly of obtaining full accreditation prior to initial operations. The high level process consists of several iterative, interdependent steps. The scope and specific activities of each step depend upon the system being certified and accredited.

a. Step 1: Requesting Accreditation. All requests for accreditation or to initiate the accreditation process will be sent to the DAA. The requesting organization will prepare and enclose an initial Computer Security Plan (see figure 3-1), appointment letters of officials assigned to information system

security duties, Certification Checklist, and list of dates regarding the planned implementation (i.e., initial operating capability, final operating capability for information system, or application development). The requesting organization will forward a copy of the request to the Certification Authority.

b. Step 2: Initial DAA Action. The DAA will determine the accreditation approach to be used and forward to the Certification Authority. The Certification Authority will prepare an initial certification plan, conduct the necessary system/site security assessments, and identify personnel to perform on-site testing if deemed necessary. The Certification Authority will also assess the relevance and utility of existing security documentation. For new developments, or in operational environments where security documentation does not exist or is not adequate to support the certification effort, the organization will prepare an SSAA in lieu of a separate Computer Security Plan, Concept of Operations, Certification Test Plan, Security Test and Evaluation Test Plan and Procedures, Contingency Plan, and the description of the environment's hardware and software. The certification plan will also describe any requirements for additional documentation other than those described in Step 3 and will tentatively assign a timeframe for conducting the certification. The certification plan will be forwarded to the DAA for approval. Once approved, the certification plan will be sent to the requesting organization to be used as a guideline in their effort to receive an accreditation.

c. Step 3: Preparing for Certification. The organization will begin preparing for certification.[1] The requesting organization, with guidance from the CISS, will:

(1) Implement a process to manage risk. (Past efforts, to precisely measure risk, have resulted in the expenditure of considerable resources [i.e., time, money, people] to perform formal risk analyses, of which the outcome has not be resulted in improved security. Therefore, Appendix III of authority document OMB Circular A-130, advises that efforts are best directed towards generally assessing risks and taking prudent measures to manage them. FIPS Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, provides guidance regarding risk management [specifically risk assessment and risk mitigation]. Organizations will either select the process described in the FIPS Special Publication to identify risk or use the DISA developed Expert Systems for Progressive Risk Identification techniques [ESPRIT]. Regardless of the effort, the end result will be in a concept document which discuses how risks will be managed in the operational environment

[1] Completion of the items identified in Step 3 is required before the organization proceeds to Step 4. The organization's statement is recognition that all efforts required to support certification have been completed.

and identifies the procedures to be used.)

(2) Prepare a Statement of Compliance with the Security Requirements in chapter 2. (The requesting organization must state that it has complied with the minimum security requirements described in chapter 2.)

(3) Prepare a Security Plan[2] (see figure 3-1).

(4) Prepare a Concept of Operations that discusses system security features and provides diagrams of network connectivity.

(5) Prepare a System User's Guide (with a chapter dedicated to a discussion of the security features designed and developed into the system for the user's awareness).

(6) Prepare a Configuration Management Plan. (This is a minimum requirement for site certification.)

(7) Submit appointment letters of the responsible Information System Security Officials.[3]

(8) Execute any Memorandums of Agreement or Understanding or obtain appropriate connection approvals, as required in DoDD 5200.28.

(9) Prepare a Certification Test Plan. (The plan will address the conduct of both the technical and nontechnical features to be tested.)

(10) Prepare a Security Test and Evaluation Plan and Test Procedures.

(11) Prepare a Contingency Plan.

(12) Prepare local SOPs.[4]

(13) Complete the Certification Checklist.

(14) Prepare a written Physical Description of the Hardware and Software.[5]

(15) Prepare the organization's statement that the information processing asset is ready for certification.

---

[2] Minimum required documents for the approval of workstations (i.e., personal computers, laptops, and notebooks) processing classified or sensitive, but unclassified information in a standalone (without connectivity) mode.

[3] See Footnote No. 2.

[4] See Footnote No. 2, Pg. 3-6.

[5] See Footnote No. 2, Pg. 3-6.

d. Step 4: Certification. The Certification Authority, along with assistance from the requesting organization, will conduct certification testing. The Certification Authority will determine the depth and breath of certification and the type of evaluation that will take place. Certification involves an assessment of the list of documentation described in Step 2, along with the requirements described in chapter 2. The Certification Authority will prepare, at the conclusion of the certification effort, a certification report. The certification report will be sent to the requesting organization for comment and a recommendation in support of an accreditation decision to the DAA.

e. Step 5: Resolution of Certification Test Findings. The Certification Authority will forward the list of categorized findings and a recommendation to the requesting organization for resolution. If the Certification Authority has recommended that a statement of accreditation or termination be issued, the certification report will go directly to the DAA with a copy to the requesting organization. If the Certification Authority has recommended an IATO, the requesting organization will have 30 working days to respond to the findings. The organization will prepare a response that describes its plan to correct the findings, provides milestone dates for correction, and cites the allocated resources (i.e., personnel and money) to be used to correct the deficiencies. If the Certification Authority has recommended termination, the organization will take immediate action to cease operations after receipt of the letter from the DAA.

f. Step 6: Accreditation Decision. The DAA will review the recommendation presented and make an accreditation decision. An accreditation is effective for 3 years from the date signed. For an IATO, the requesting organization will have 180 days from the date that the DAA issued the IATO to correct the deficiencies. No more than one extension to the first IATO will be granted without sufficient justification. The DAA will make an accreditation decision based on the recommendation of the Certification Authority and the results documented in the certification report. Any conditions required to maintain acceptable levels of risk will be established through the formal accreditation decision correspondence from the DAA to the requesting organization.

g. Step 7: Maintenance of the Accredited Baseline. The statement of accreditation describes the definitive baseline of security operations with an acceptable level of risk. A statement of accreditation does not obviate the responsibility of the site for managing the accredited baseline. Therefore, the organization ISSM or ISSO will maintain the accredited baseline using and approved configuration management process and will perform an annual assessment of the baseline. The responsible ISSM or ISSO will maintain overall responsibility for retaining and maintaining records on the accreditation decisions

for systems and networks under their purview. The responsible ISSM or ISSO will periodically evaluate the accredited status and will make a determination if reaccreditation is needed (as described in paragraph 3 of this chapter). If reaccreditation is not needed, the ISSM or ISSO will document the scope and date of the review performed and will maintain a file of the reviews conducted. As a secondary measure, CISS, operating under the DAA's authority, will periodically measure the effectiveness of the accredited baseline via the use of compliance validation tools.

7. DISA System Security Plan. An SSP is required for all DISA information systems. Figure 3-1 provides a sample security plan that conforms to the requirements identified in Appendix A of OMB Bulletin No. 90-08 (reference 4c) and the U.S. Department Of Commerce Guidelines for Developing and Evaluating Security Plans for Sensitive and Classified Systems, June 1992. Where applicable, references to guidelines in OMB Bulletin No. 90-08 are shown in brackets { }. All DISA activities will use this format when submitting their SSPs. Section IV of the DISA SSP titled, Additional Comments, will be used to identify proposed safeguards for systems under development or modification methods used to ensure that up-front security requirements will be met.

a. Exemptions. Request for SSP exemptions will be submitted by the ISSO through the ISSM to the DISA CISSM. Specific, written justification must accompany all such requests.

b. Safeguarding. A completed SSP will be considered to be at least sensitive but unclassified information and will be marked and safeguarded appropriately. A completed SSP for systems that process classified information will be marked and safeguarded in a manner consistent with the classification level and sensitivity of the system in question. If the SSP is classified, the classification level of each paragraph and section must be indicated. Where feasible, classified SSP data should be supplied on a separate attachment and referenced appropriately.

SECTION II (CON.)		
C. RISK INDEX DETERMINATION (PER ENCLOSURE 4 of DoDD 5200.28).		
Minimum User Clearance (Table 1)	**TS S C S/U None**	**Rating (Rmin):**
Maximum Data Sensitivity (Table 2)	**TS S C S/U U**	**Rating (Rmax):**
Categories	**List:**	**Count:**
Risk Index, Mode, Class (Table 3)	**Security Mode:** **Min. Security Class:**	**Risk Index:**
D. ENVIRONMENT		
Development/Maintenance Environment	1. High level architectural view.	
	2. Responsible organization and location.	
Target/Operational Environment	1. High level architectural view.	
	2. Hardware/software suite (high level).	
Threat/Vulnerability/Risk Factors		

SECTION III. SYSTEM SECURITY MEASURES		
A. RISK ASSESSMENT AND MANAGEMENT {III.A, III.B, III.C}		
Risk Assessment Status	*COMPLETED* on _____ (Date) by _____ (Name/Org)	*PENDING* _____ Start Date _____ Est. Completion Date
Methodology {III.B}	__ Formal Risk Analysis	__ Other (Explain in Section IV)
Applicable Guidance*** {III.B}		

*** Specific regulations, guidance used in the design, implementation, or operation of the protective measures used on the system. This should include Department and Agency policy/guidance documents such as DODD 5200.28 and this Instruction.

FIGURE 3-1. SYSTEM SECURITY PLAN (CON.)

SECTION III (C)

B. SYSTEM SECURITY CONTROL MEASURE STATUS {III.C}

The "M/G" column indicates applicability to Major Applications (M) and/or General Support Systems (G).

Indicate dates in "In Place" or "Planned" columns, as applicable. Show "est." for estimated dates.

- If "In Place", provide specifics or reference appropriate document in REMARKS.
- For controls that are not needed, cost effective, or appropriate, indicate N/A and reason (e.g., "no financial data on system") in REMARKS.
- If measures are partially in-place and/or changes are planned, indicate both "In-Place" and "Planned".
- If "Planned", identify measures and projected operational date.
- If additional space is required, use Section IV and reference in REMARKS.

M/G			IN PLACE	PLANNED	REMARKS
		1. Management Controls			
M	G	Assignment of Security Responsibility			
	G	Risk Analysis/Sensitivity Assessment			
M	G	Personnel Selection/Screening			
		2. Acquisition/Development/ Installation Controls			
	G	Acquisition Specifications (HW/SW)			
M		Security Specifications			
M		Design Review and Testing			
M	G	Certification			
M	G	Accreditation			
		3. Operational Controls			
M	G	Physical and Environmental Protection			
M	G	Production, I/O Controls			
M	G	Emergency, Backup and Contingency Planning			
		Disaster Recovery Planning			
M	G	Audit and Variance Detection			
M		Application S/W Maintenance Controls			
	G	Hardware and System S/W Maintenance Controls			
M	G	Documentation			
		4. Security Awareness and Training			
M	G	Security Awareness and Training Measures			
		5. Technical Controls			
M	G	User Identification and Authentication			
M	G	Authorization/Access Control			
M	G	Integrity/Validation Controls			
	G	Confidentiality Controls			
M	G	Audit Trails and Journaling			
-	-	Availability Controls****			

**** Added controls (to reduce denial of service risks and ensure continued system availability) apply to M and G.

FIGURE 3-1. SYSTEM SECURITY PLAN (CON.)

DEFENSE INFORMATION SYSTEMS AGENCY
INFORMATION SYSTEM SECURITY PLAN
[Effective Date of Plan]

SECTION II. BASIC SYSTEM IDENTIFICATION

A. Responsible Organization (Subcomponent with full address) {I.A}		
B. System Name/Title {I.B}		
C. System Category {I.C}	Major Application	General Support System
D. System Operational Status {I.D}	Operational	Under Development/Modification Operational Date _____
E. General Description / Purpose {I.F}		
F. System Security Environment and Special Considerations (e.g., Periods Processing) {I.F}		
G. Point(s) of Contact {I.G}		
H. Level of Aggregation	Single identifiable system	Group of similar systems*
I. Connectivity	Standalone	Connected (List in Remarks)
J. Accreditation Status Show conditions or caveats in Section IV.	*Accredited* by (DAA) on (Date)	*NOT Accredited* Request Submitted to (DAA) on (Date)
K. Security Mode(s) of Operation	Dedicated System High	Multilevel/Partitioned Multilevel

* Systems under the same management control with essentially the same function, reside in the same environment and have the same security characteristics and needs.

SECTION III. SENSITIVITY OF INFORMATION

A. Applicable Laws or Regulations {II.A}**	Privacy Act: **Y/N** If so, Used for Matching Activities?: **Y/N** List Others:
B. General Description of Information Sensitivity {II.B}	
Classification/Sensitivity %	TS S C S/U U
Confidentiality H M L	
Integrity H M L	
Availability H M L	

** List laws or regulations that establish specific requirements for confidentiality, integrity, or availability of information (e.g., E. O. 12958, Classified National Security Information, 17 April 1995, DOD 5200.1-R [reference 4a], DISAI 240-110-8 [reference 4b]). Do not list those describing protection requirements for systems (e.g., DODD 5200.28).

FIGURE 3-1. SYSTEM SECURITY PLAN

SECTION IV. ADDITIONAL COMMENTS Reference Security Plan section and paragraph where appropriate.
o Note any relevant feature of the system security environment such as any evaluated product used. o Note any relevant feature of the system environment such as intended use of periods processing. o For small systems, list hardware (make and model) and software (name and version.) This is the baseline for accreditation. o For a preliminary security plan being submitted with a request for accreditation, provide a schedule that addresses, at a minimum, the target date for accreditation (operation) and an estimated date that the system will be ready for certification.

FIGURE 3-1. SYSTEM SECURITY PLAN (CON.)

PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4. SECURITY AWARENESS, TRAINING, AND PROFESSIONALIZATION

1. General. Within DISA there are three distinct information systems security training categories: (1) general awareness and training, (2) system specific training, and (3) professionalization training.

2. General Awareness And Training. General awareness and training provides an understanding of: DISA policy and goals for protecting information and information systems, the roles and responsibilities of the various security staff personnel, and the relationship between information systems security and other security disciplines. General awareness and training sensitizes personnel to the existence of potential threats and vulnerabilities associated with the use of information systems. Training also heightens awareness of the need to protect data, information, and information system assets. All personnel should be trained in the areas outlined below as well as those areas identified in table 4-1.

a. Initial and Recurring Training.

(1) Initial. Newly assigned personnel will receive security training prior to being granted access to DISA information.

(2) Periodic. All personnel will receive security training on an annual basis.

(3) Refresher. Refresher security training will be provided as needed whenever there has been a change in security requirements.

b. Content. Briefing and training content should be based on the following list of topics derived from National Institute of Standards and Technology (NIST) guidelines and supplemented by any others deemed necessary by the CISSM.

(1) Understanding the roles of various DISA organizational units in ensuring adequate security and safety of information resources.

(2) Understanding DISA policy and goals for protecting data and information, to include a discussion of security violations and incidents.

(3) Working at home.

(4) Dial-in access.

(5) Connection to the Internet.

(6) Unofficial use of government equipment.

(7) Designation of sensitive data, applications, and systems.

(8) Reporting violations, infractions, or incidents.

(9) Marking, accountability, transmitting, destruction, and disclosure of sensitive data.

3. Information System Specific. Personnel must also receive security training on each specific system to which they have access. Personnel must have a clear understanding of the threats to and vulnerabilities of the system. This includes a definition of terms, a discussion of the major categories of threats (e.g., unauthorized accidental or intentional disclosure, modification, destruction, or delay), a discussion of threat impact areas, common examples of computer abuse, and examples of common system vulnerabilities.

a. Initial and Recurring Training.

(1) Initial. Newly assigned personnel will receive system specific training prior to being granted access to the information system.

(2) Periodic. All personnel will receive system specific training on an annual basis.

(3) Refresher. Refresher security training will be provided as needed whenever there has been a change in the system, system rules, or user procedures.

b. Content. The amount and depth of training needed will depend upon the specific duty requirements and expertise of the individual to be trained. The overall content will be determined by the ISSO in coordination with the System Programmer, Executive Software Group, or anyone involved in the day-to-day operation of the system in question. The briefing should contain specifics in the areas of:

(1) Assignment and limitations of privileges.

(2) Restoral activities.

(3) Cognizant security staff.

(4) Information system accreditation.

(5) Risk assessments.

(6) Security controls.
(7) Viruses and malicious logic protection.

(8) Contingency planning.

(9) Data sensitivity and protection requirements.

4. Professionalization Training. Professionalization training is primarily aimed at the security staff and provides the skills necessary to evaluate computer security procedures and practices. Professionalization training ensures that the security staff is able to apply security concepts while performing the tasks that relate to their particular positions. This training should be given in addition to the training outlined above.

a. Continuous Training. ISSMs, ISSOs, and TASOs must be knowledgeable on current Federal and DISA policies. Additionally, they must be trained on their specific local security policies, requirements, and procedures.

b. Content. Professionalization training should address the areas outlined below as well as those areas identified in table 4-2.

(1) Computer security basics.

(2) Good computer security practices.

(3) Roles of various organizations in ensuring adequate security and safety of information and information system resources.

(4) Basic concepts of risk management.

(5) Security planning.

(6) Auditing and monitoring.

(7) Information system security disciplines.

(8) Contingency planning.

(9) Life-cycle management.

GENERAL SECURITY AWARENESS
- Security Program Rationale
- Scope of Information System Abuse
- Scope of Information System Security
- Information Classification & the Law
- Applicable Regulations & Directives
- Categories of Security
- Interdisciplinary Approach
- Information System Security Plans

USER SECURITY
- User Security Responsibilities
- Risk in Information System & Facility Operations
- Countermeasures
- Password Controls

SECURITY ADMINISTRATION
- Organizing the Security Responsibilities
- Security Implementation Plans
- Security Work Flow Control
- Personnel Practices & Responsibilities

SECURITY VIOLATION REPORTING
- Identification of Appropriate Reporting Officials
- Time-Critical Reporting Requirements
- Reporting Information System Abuse Violations
- Documenting Information System Abuse Violations

CONFIGURATION MANAGEMENT
- Facility
- Hardware
- Software
- Telecommunications
- Data Sensitivity
- Human Resources
- Software Security Documentation

SOFTWARE SECURITY
- Operating Systems
- Application Systems
- Utility Routines
- Access Control and Authorization
- Detecting Attempted Violations
- Additional Software Functions
- Real Time Software Auditing
- Software Configuration Management

TELECOMMUNICATION SECURITY
- Dial Up
- Point to Point
- Local and Wide Area Networks
- Encryption
- Transmission Media Vulnerabilities

TERMINAL/WORKSTATION SECURITY
- Access to Terminals/Output
- Access to Computers/Files
- Access to Communications Lines
- Workstation Protection
- Workstation Identification

SYSTEM DESIGN SECURITY
- Project Initialization
- Investigative Study
- Generalized System Design
- Detailed System Design
- File Access Processing
- Implementation Planning
- Systems Implementation
- Post Implementation Evaluation

HARDWARE SECURITY
- Firmware
- Emanation Protection
- Encryption Devices
- COMSEC (Communications Security)

PHYSICAL SECURITY
- Building Design & Protection
- Emanation Protection
- Electric Power
- Fire Protection
- Air-Conditioning
- Floods, Earthquake, Windstorm
- Housekeeping
- Alternative & Emergency Backup Facilities
- Access

PERSONNEL SECURITY
- Personnel Selection and Hiring Procedures
- Personnel Control
- Job Rotation Program
- Security Awareness Training Program
- Background Investigation
- Access and Clearances
- Screening Techniques
- Security Briefing
- Disciplinary Actions
- Substance Abuse

TABLE 4-1. TRAINING SUBJECT AREAS

General Security Awareness	An overview of the scope of computer abuse, DISA Information Systems Security Program, laws, regulations, and procedures for establishing and executing an activity's information system security program.
User and Customer Security	The user's risk associated with receiving information system services and determining responsibility and protection requirements for user data security and integrity.
Security Administration	All parts of information system security program administration, implementation, risk management, and contingency planning, and their interrelationships.
Security Violation Reporting	Reporting security violations to the appropriate DISA officials.
Configuration Management	Procedures for managing any change to the information system configuration.
Software Security	Includes all types of application, operating systems, software controls, and countermeasures that can reduce the threats associated with processing different levels of data.
Telecommunication Security	Identification of all of the telecommunications safeguards available to reduce the threats associated with transmitting different levels of data.
Terminal and Device Related Security	The controls and countermeasures that the user and customer must adhere to in order to protect data.
Systems Design Security	The controls and countermeasures that must be built into the design of an information system application to meet the level of security the user and customer require.
Hardware Security	Identification of the controls and countermeasures available to reduce the threats associated with processing different levels of data. In addition, the differences between hardware and software countermeasures must be evaluated and discussed.
Physical Security	The security requirements and countermeasures for physical protection of all information system resources.
Personnel Security	The personnel security requirements associated with human resources when performing information system operations.

4-2. PROFESSIONALIZATION TRAINING REQUIREMENTS

Computer Auditing	Auditing principles, methods, tools, techniques, and responsibilities required for the periodic examination and evaluation of the computer system procedures, controls, and data.
Information Security	Identification of the levels and types of data and the appropriate countermeasures to protect the data.
Risk Assessment Methodology	The steps associated with conducting an activity Risk Assessment and selecting cost-effective countermeasures to protect information system assets.
Contingency and Backup Planning	Identification and documentation of a systematic method of response to any type of information system operation disruption or emergency situation.
Information System Security and DISA Contractors	The interface between Industrial Security regulations, Defense Intelligence Agency regulations, Defense Information Systems Agency instructions, and National Security Agency regulations, which must be reconciled during the information system accreditation process.
Disaster Recovery	The requirements and procedures to develop an activity disaster recovery plan for information system resources.
Security Accreditation	The security review, certification, and approval requirements and steps that must be taken to have an information system accredited.
Security Test and Evaluation	Identification and documentation of a systematic method for testing all the security countermeasures associated with information systems and determining if all required countermeasures are being utilized.

TABLE 4-2. PROFESSIONALIZATION TRAINING REQUIREMENTS (CON.)